UNITED STATES DISTRICT COURT

FOR THE WESTERN DISTRICT OF NEW YORK

IN RE: PRACTICEFIRST DATA BREACH LITIGATION	Civil No. 1:2021-cv-00790-JLS **CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs, PETER TASSMER, KAREN CANNON, PAUL COMMISSO, and GLENDA JOHNSON, individually, and on behalf of all others similarly situated, on personal knowledge of the facts pertaining to them and on information and belief as to all other matters, by and through the undersigned counsel, hereby bring this Consolidated Class Action Complaint against Defendant Professional Business Systems d/b/a Practice*first* Medical Management Solutions and PBS Medcode Corp. (collectively "Practice*first*" or "Defendant"), and allege as follows:

INTRODUCTION

1. This class action arises out of the recent data breach exposing confidential information in the possession and control of Practice*first*.

2. Practice*first* is a medical management solutions company that touts itself as a "leader in billing, credentialing, coding, compliance, chart auditing, bookkeeping and tax preparation."[1]

3. Practice*first* provides administrative and back–office services to medical professionals and takes "responsibility to stay current with the volatile rules, regulations and information technology requirement of the healthcare industry."[2]

[1] https://www.practice*first*secure.com/about
[2] *Id.*

4. On December 30, 2020, Practice*first* "discovered" that, because of their unsecure and inadequate data security practices and procedures, an unauthorized third party accessed and exfiltrated files from their computer system, including patient and employee data (the "Data Breach") for over 1.2 million individuals. It is unclear how long this unauthorized access and exfiltration went on before being discovered.

5. Although the information accessed and stolen varies by individual, the categories of patient and employee data obtained by the hackers included: names, addresses, email addresses, dates of birth, driver's license numbers, Social Security numbers, diagnoses, laboratory and treatment information, patient identification numbers, employee username and passwords, employee username with security questions and answers, and bank account and/or credit card/debit card information.[3] Collectively, this information is known as Protected Healthcare Information ("PHI") and Personally Identifiable Information ("PII"), and this information is of significant value to and sought after by cyber criminals.

6. On July 1, 2021—over six months after discovering the Data Breach—Practice*first* notified the Attorneys General of several states, including Maine and California, of the breach. Around the same time, Practice*first* also began sending notices to patients and employees whose PII/PHI may have been impacted by the Data Breach.

7. Due to Practice*first's* carelessness and inadequate data security, Plaintiffs and over 1.2 million other individuals have suffered irreparable harm and are subject to an increased risk of identity theft because their PII/PHI has been compromised and they must now undertake additional ongoing security measures to minimize the risk of identity theft.

[3] https://www.practice*first*secure.com/security-incident

PARTIES

8. Plaintiff Peter Tassmer resides in the City of New Britain and is a citizen of the State of Connecticut.

9. Plaintiff Karen Cannon resides in the City of Dunkirk and is a citizen of the State of New York.

10. Plaintiff Paul Commisso resides in the City of Akron and is a citizen of the State of the State of New York.

11. Plaintiff Glenda Johnson resides in the City of Buffalo and is a citizen of the State of New York.

12. Defendant Professional Business Systems, Inc., d/b/a Practice*first* Medical Management Solutions and PBS Medcode Corp. is a New York corporation, headquartered in New York. Its principal place of business is at 275 Northpointe Parkway, Suite 50, Amherst, NY, 14228. It serves over 75 physician practices across the country and, consequently, maintains on its server network PII/PHI for individuals who are patients of their clients from states other than the State of New York.

JURISDICTION AND VENUE

13. The Court has subject matter jurisdiction over this case pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because at least one member of the proposed class is a citizen of a state different from the Defendant's home state, the number of proposed class members exceeds 100, and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs.

14. The Court has personal jurisdiction over Defendant because it conducts business in New York and is incorporated and headquartered in New York.

15. Venue is also proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendant resides in this district and regularly conducts business in this district, a substantial part of the events and/or omissions giving rise to Plaintiffs' and the Class members' claims occurred within this district, and Defendant has caused harm to class members residing in this district.

FACTUAL ALLEGATIONS

16. As a medical management solutions business focused on the efficiency, accuracy, and security of the data it processes for health care providers, Practice*first* has both the duty and the means to provide secure systems for the sensitive healthcare billing and coding services it provides.

17. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class members' PII/PHI, Defendant assumed legal and equitable duties to those individuals. Additionally, Defendant acknowledged its responsibilities for protecting Plaintiffs' and Class members' PII/PHI from unauthorized access, disclosure, and exfiltration in its privacy statement, which expressly states it is provided patient PII/PHI—which includes the Plaintiffs' and Class members' information at issue here—that constitutes health information protected by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), that it is a Covered Entity under HIPAA, and that it complies with HIPAA's PII/PHI disclosure regulations.[4] Plaintiffs and the Class had a reasonable expectation that Practice*first* would secure the information it processed and maintained.

18. On December 30, 2020, Defendant "discovered" that an unauthorized actor had accessed its computer system and copied (exfiltrated) files.[5]

---

[4] *Privacy Policy*, Practice*first*, https://www.practice*first*secure.com/privacy (last accessed October 15, 2021)

[5] *Notice of Security Incident*, Practice*first*, https://www.practice*first*secure.com/security-incident (last accessed Aug. 9, 2021)

19. Defendant engaged a forensic investigation firm to determine the nature and scope of this incident. Defendant determined the Data Breach resulted from an unknown individual or individuals outside of its organization gaining access to its network, including where Defendant stored files containing employee information and the confidential patient information of its clients.[6]

20. Defendant's investigation further determined that, as a result of this incident, certain PII and PHI was compromised, including names, addresses, email addresses, dates of birth, driver's license numbers, Social Security numbers, diagnosis information, laboratory and treatment information, patient identification numbers, medication information, health insurance identification and claims information, tax identification numbers, and bank account and/or credit/debit card information.[7] The investigation also revealed that 1,210,688 individuals were impacted by the Data Breach.[8]

21. On or about June 30, 2021, Plaintiffs and Class members were belatedly notified their PII/PHI had been accessed and "copied by an unauthorized actor before it was permanently deleted," according to the notice submitted to the Office of the Attorney General for the State of California on or about July 1, 2021. This delay in notification to Plaintiffs and Class members gave the unauthorized party ("hackers") time to use the stolen PII/PHI without restriction, further harming Plaintiffs and Class members.

---

[6] *Id.*
[7] *Id.*
[8] *See Cases Currently Under Investigation*, Office for Civil Rights, U.S. Dept. of Health and Human Services, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Aug. 9, 2021).

22. Even if the unauthorized party later claimed they deleted the exfiltrated PII/PHI, computer experts have definitively stated that "Proof of deletion is not a thing."[9] There is simply no way Defendant could possibly know if the hackers did not simply copy exfiltrated PII/PHI to another location before offering whatever "proof" the unauthorized party may or may not have claimed to have showed that the original copy of the data was deleted. If Defendant put its trust in the very person/people responsible for the Data Breach in the first place, its trust is unfounded—and does not in any way absolve Defendant of its statutory responsibilities to prevent the unauthorized access and exfiltration PII/PHI.

23. Defendant has obligations and duties created by HIPAA, industry standards, and common law to keep Plaintiffs' and Class members' PII/PHI confidential and to protect it from unauthorized access, disclosure, and exfiltration.

24. Defendant violated HIPAA because, as a medical billing, coding, and management services provider, it is required to secure and protect Plaintiffs and Class members' PII/PHI, because they are "protected health information" as defined under 45 CFR § 160.103. And this information was breached as defined by 45 CFR § 164.402: "the acquisition, access, use, or disclosure of protected health information in a manner not permitted."

25. Defendant violated statutory requirements and breached its duties by failing to protect Plaintiffs and Class members because it did not employ the required appropriate security to detect intrusions, thus allowing the hackers to steal the most private and sensitive information belonging to Plaintiffs and Class members. Plaintiffs and Class members reasonably believe the risk of future harm (including identity theft) is substantial, imminent, and likely, and they need to take steps to mitigate that substantial risk of future harm. At a minimum, Plaintiffs and Class

[9] *See* Keith Mukai, *ArbiterSports Was Hacked. Don't Use Them Ever Again*, Medium (Aug. 29, 2020), https://medium.com/@kdmukai_64726/arbitersports-was-hacked-dont-use-them-ever-again-fddea92bcd21 (last accessed Aug. 9, 2021)

members must now and in the future closely monitor their financial accounts to guard against identity theft.

26. Accordingly, Plaintiffs brings this action against Defendant seeking redress for its unlawful conduct and assert claims for negligence, breach of contracts to which Plaintiffs and Class members are third-party beneficiaries, and declaratory relief. Plaintiffs seek remedies including compensatory damages, reimbursement of out–of–pocket costs, and injunctive relief, including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

A. Plaintiffs' Experiences, Injuries, and Damages.

27. Plaintiff Tassmer received notice of the Data Breach on or about July 3, 2021. The letter from Practice*first* instructed Plaintiff Tassmer to, among other things, "regularly review account statements and report any suspicious activity to financial institutions." It also provided him an option to enroll in credit monitoring and identity theft recovery services.

28. After receiving the Notice letter, Plaintiff Tassmer made reasonable efforts to mitigate further impact of the Data Breach. He spent time researching the Data Breach and reviewing and monitoring his credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. This is valuable time he otherwise would have spent on other activities.

29. Plaintiff Tassmer suffered additional actual injury from having his PII/PHI compromised in the Data Breach including (a) damage to and diminution in the value of his PII, a form of property that Defendant had possession of; (b) violation of his privacy rights; and (c) further imminent and impending injury arising from the increased risk of identity theft, and financial and medical fraud.

30. Plaintiff Cannon received notice of the Data Breach on or about July 3, 2021. The letter from Practice*first* instructed Plaintiff Cannon to, among other things, "regularly review account statements and report any suspicious activity to financial institutions." It also provided her an option to enroll in credit monitoring and identity theft recovery services.

31. After receiving the Notice letter, Plaintiff Cannon made reasonable efforts to mitigate further impact of the Data Breach. She spent time researching the Data Breach, reviewing and monitoring her credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. This is valuable time she otherwise would have spent on other activities.

32. Plaintiff Cannon suffered additional actual injury from having her PII/PHI compromised in the Data Breach including (a) damage to and diminution in the value of her PII/PHI, a form of property that Defendant had possession of; (b) violation of her privacy rights; and (c) further imminent and impending injury arising from the increased risk of identity theft, and financial and medical fraud.

33. Plaintiff Commisso received notice of the Data Breach on or about June 30, 2021. He takes measures to protect his PII/PHI and is very careful about sharing his PII/PHI. He has never knowingly transmitted unencrypted PII/PHI over the internet or any other unsecured source. The letter from Practice*first* instructed Plaintiff Commisso to, among other things, "regularly review account statements and report any suspicious activity to financial institutions." It also provided him an option to enroll in credit monitoring and identity theft recovery services.

34. After receiving the Notice letter, Plaintiff Commisso made reasonable efforts to mitigate further impact of the Data Breach. He spent time researching the Data Breach, reviewing and monitoring his credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. This time included time spent on the telephone and

sorting through unsolicited spam, verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft insurance options, and self–monitoring his sensitive accounts. This is valuable time he otherwise would have spent on other activities.

35. Plaintiff Commisso suffered additional actual injury from having his PII/PHI compromised in the Data Breach including (a) damage to and diminution in the value of his PII/PHI, a form of property that Defendant had possession of; (b) violation of his privacy rights; and (c) further imminent and impending injury arising from the increased risk of identity theft, and financial and medical fraud.

36. Plaintiff Johnson received notice of the Data Breach on or about June 30, 2021. He takes measures to protect his PII/PHI and is very careful about sharing his PII/PHI. He has never knowingly transmitted unencrypted PII/PHI over the internet or any other unsecured source. The letter from Practice*first* instructed Plaintiff Johnson to, among other things, "regularly review account statements and report any suspicious activity to financial institutions." It also provided him an option to enroll in credit monitoring and identity theft recovery services.

37. After receiving the Notice letter, Plaintiff Johnson made reasonable efforts to mitigate further impact of the Data Breach. He spent time researching the Data Breach and reviewing and monitoring his credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. This time included time spent on the telephone and sorting through unsolicited spam, verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft insurance options, and self–monitoring his sensitive accounts. This is valuable time he otherwise would have spent on other activities.

38. Plaintiff Johnson suffered additional actual injury from having his PII/PHI compromised in the Data Breach including (a) damage to and diminution in the value of his PII/PHI, a form of property that Defendant had possession of; (b) violation of his privacy rights;

and (c) further imminent and impending injury arising from the increased risk of identity theft, and financial and medical fraud.

39. Due to the Data Breach, Plaintiffs each anticipate spending additional time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach—including spending time on the telephone dealing with fraud attempts, sorting through unsolicited spam, and self–monitoring their private and sensitive accounts.

B. Plaintiffs' and Class Members' PII/PHI Was Also Subject to a Ransomware Attack—a Distinct Form of Data Breach.

40. A ransomware attack is a type of malicious software that blocks access to a computer system or data, usually by encrypting it, until the owner pays a fee to the perpetrator.

41. Ransomware attacks are considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, ". . . the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40.

42. Also, in a ransomware advisory, the Department of Health and Human Services informed entities covered by HIPAA that "when electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information)."[10]

43. Ransomware attacks also constitute data breaches in the traditional sense. For example, in a ransomware attack on the Florida city of Pensacola, and while the City was still

[10] *See Fact Sheet: Ransomware and HIPAA*, Health and Human Services, https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf (last accessed August 9, 2021).

recovering from the ransomware attack, hackers released 2GB of data files from the total 32GB of data that they claimed was stolen prior to encrypting the City's network with the maze ransomware. In the statement given to a news outlet, the hackers said, "***This is the fault of mass media who writes that we don't exfiltrate data*** . . . ."[11]

44. Other security experts agree that when a ransomware attack occurs, a data breach does as well, because such an attack represents a loss of control of the data within a network.[12]

45. Ransomware attacks are also Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

> The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. See 45 C.F.R.164.308(a)(6).[13]

46. The ransomware attack on Defendant included Plaintiffs' and Class members' PII/PHI stored on Defendant's computer system. As part of the Defendant's notice to Plaintiffs and Class members about the ransomware attack and Data Breach, Defendant stated Plaintiffs' and Class members' PII/PHI was copied by the unauthorized actor. Therefore, an unauthorized

---

[11] *Pensacola Ransomware: Hackers Release 2GB Data as a Proof*, Cisomag (Dec. 27, 2019), https://www.cisomag.com/pensacola-ransomware-hackers-release-2gb-data-as-a-proof/ (emphasis added)

[12] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019). Available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

[13] *Supra,* note 10.

party now possesses Plaintiffs' and Class members' PII/PHI because, as previously stated, "Proof of deletion is not a thing."[14]

C. Defendant Knew or Should Have Known the Risk of a Data Breach Because the Healthcare Sector is Increasingly Targeted by Hackers.

47. Healthcare related data breaches continue to rapidly increase. According to the 2019 HIMSS Cybersecurity Survey, 82 percent of participating hospital information security leaders reported having a significant security incident within the previous 12 months, and most of these *known* incidents being caused by "bad actors," such as cybercriminals.[15] "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[16]

48. As industry service providers handling PII/PHI, Defendant knew, or should have known, the importance of safeguarding PII/PHI entrusted to them, and of the foreseeable consequences if their data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class members as a result of a ransomware attack and/or data breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

49. Defendant knew and understood unprotected or exposed PII/PHI in the custody of healthcare entities and their service providers, such as Defendant, is valuable and highly sought

[14] *See* Keith Mukai, *ArbiterSports Was Hacked. Don't Use Them Ever Again*, Medium (Aug. 29, 2020), https://medium.com/@kdmukai_64726/arbitersports-was-hacked-dont-use-them-ever-again-fddea92bcd21 (last accessed Aug. 9, 2021)

[15] *2019 HIMSS Cybersecurity Survey, available at*: https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last accessed June 7, 2021).

[16] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last accessed June 7, 2021).

after by nefarious third parties seeking to illegally monetize that PII/PHI through unauthorized access and exfiltration. In fact, the healthcare sector reported the second largest number of data breaches among all measured sectors in 2018, with the highest rate of exposure per breach.

50. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. Medical identity theft is one of the most common forms of identity theft, most expensive, and most difficult to prevent. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which is more "than identity thefts involving banking and finance, the government and the military, or education."[17]

51. A report focusing on healthcare breaches found the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that victims were often forced to pay out of pocket costs for healthcare they did not receive in order to restore their coverage. Almost 50 percent of the victims lost their healthcare coverage because of the fraud–related incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft. Data breaches and identity theft have a crippling effect on individuals, and detrimentally impacts the economy as a whole.

52. Medical data, like Plaintiffs' and Class members' PII/PHI, is also especially valuable to identity thieves. As indicated by Jim Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals – they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one

[17] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last visited July 7, 2021).

place."[18] According to a report by the FBI's Cyber Division, healthcare records can be sold by criminals for 50 times the price of stolen Social Security numbers or credit card numbers.[19] For example, credit card information and associated personal information can sell for as little as $1-$2 on the black market according to the Infosec Institute.[20] Whereas a file containing private health insurance information can be bought for between $1,200 and $1,300 ***each*** on the black market.[21]

53. PII/PHI is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information for a number of years on the "cyber black-market," commonly referred to as the dark web. As a result of large–scale data breaches, identity thieves and cyber criminals have openly posted stolen Social Security numbers, healthcare information, and other PII/PHI directly on various Internet websites making the information publicly available. These networks and markets consist of hundreds of thousands, if not millions, of nefarious actors who view and access the PII/PHI.

54. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII/PHI. To protect themselves, Plaintiffs and Class members (and the business entities whose information was breached) will need to be remain vigilant against unauthorized data use for years or even decades to come.

---

[18] IDExperts, You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows, https://www.idx.us/knowledge-center/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat (last visited July 8, 2021).

[19] *FBI Cyber Division Bulletin: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusion*, FBI (Apr. 8, 2014), https://publicintelligence.net/fbi-health-care-cyber-intrusions/.

[20] *Data Breaches: In the Healthcare Sector,* Center for Internet Security, https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last visited July 28, 2021).

[21] Elizabeth Clarke, *Hackers Sell Health Insurance Credentials, Bank Accounts, SSNs and Counterfeit Documents*, SecureWorks (July 15, 2013), https://www.secureworks.com/blog/general-hackers-sell-health-insurance-credentials-bank-accounts-ssns-and-counterfeit-documents

D. Defendant Failed to Heed FTC Warnings or Comply with FTC Guidelines.

55. The Federal Trade Commission ("FTC") promulgated numerous guides for businesses highlighting the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision–making.

56. In 2016, the FTC updated *Protecting Personal Information: A Guide for Business*, its publication establishing cyber–security guidelines for businesses. These guidelines note businesses should protect the personal customer information they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[22]

57. The guidelines also recommend businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[23]

58. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

59. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and

[22] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Aug. 9, 2021).
[23] *Id.*

appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations. These FTC enforcement actions include actions against entities in the healthcare industry, like Defendant.[24]

60. The FTC also recognizes that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, a former Commissioner, Pamela Jones Harbour, underscored the point: Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency.

E. The PHI/PII Stolen in The Data Breach Is Incredibly Valuable to Criminals for Identity Theft and Fraudulent Acts.

61. The personally identifying, health, and financial information of consumers, such as Plaintiffs and Class members, is valuable and has been commoditized in recent years.

62. The repercussions of Practice*first*'s failure to keep Plaintiffs' and Class members' PII/PHI secure are severe. Identity fraud occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security Number, date of birth, and/or other information, such as health insurance or prescriptions, without permission, to commit fraud amongst other crimes.

63. According to experts, one out of four data breach notification recipients become a victim of identity fraud.

[24] *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

64. Stolen PHI/PHI is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. This is because malicious actors buy and sell that information for profit.[25] Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal identities and online activity.

65. The PII/PHI stolen here commands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[26]

66. Once PII/PHI is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional personally identifying information being harvested from the victim, as well as information from family, friends, and colleagues of the original victim.

67. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet–enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.

68. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Waiting over six months to notify Attorneys General, Plaintiffs, and Class members that the PII/PHI had been stolen is far from rapid reporting.

---

[25] *Shining a Light on the Dark Web with Identity Monitoring*, IdentityForce, Dec. 28, 2020, *available at*: https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited July 7, 2021).

[26] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited July 7, 2021).

69. Victims of identity fraud also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

70. Data breaches facilitate identity fraud as hackers obtain patients' PII/PHI and thereafter use it to perpetrate health insurance fraud, siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII/PHI to others who do the same.

71. For example, the United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use PII/PHI to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[27] The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."[28]

72. Moreover, in light of the current COVID-19 pandemic, Plaintiffs' sensitive information could be used to fraudulently obtain any emergency stimulus or relief payments or any additional forms monetary compensation, unemployment and/or enhanced unemployment benefits.

73. Victims of identity theft often suffer indirect financial costs as well, including the costs incurred due to litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit.

---

[27] *See* Government Accountability Office, Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown (June 2007), available at http://www.gao.gov/assets/270/262899.pdf (last visited July 7, 2021).

[28] *Id.*

74. In addition to out–of–pocket expenses that can exceed thousands of dollars for the victim of new account identity theft, and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their PII/PHI. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

75. The information compromised in the Data Breach here is significantly more valuable than the loss of, for example, just credit card information because there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach—names, addresses, dates of birth, driver's license numbers, Social Security numbers, diagnosis information, laboratory and treatment information, patient identification numbers, medication information, health insurance identification and claims information, tax identification numbers, and bank account and/or credit/debit card information—is difficult, if not impossible, to change.

76. Social Security numbers are among the worst kind of personal information to have stolen because they can be misused so many different ways and are very hard to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social

> Security number and assuming your identity can cause a lot of problems.[29]

77. And it is no easy task to change or cancel a stolen Social Security number. Plaintiffs and the Class members cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

78. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[30]

79. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud and bank/finance fraud. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

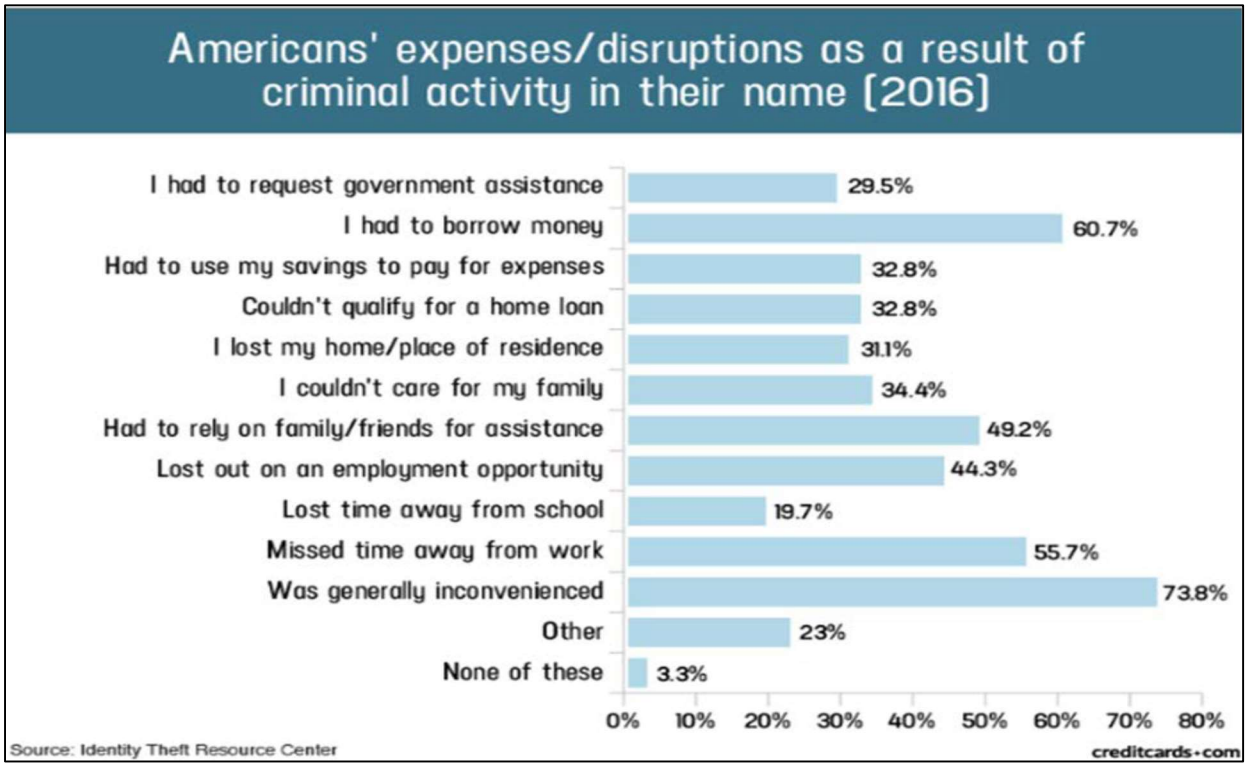
---

[29] Social Security Administration, *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 7, 2021).

[30] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited July 7, 2021).

80. According to the Federal Trade Commission ("FTC"), unauthorized PII/PHI disclosures wreak havoc on consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout.[31]

81. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[32]



82. Identity theft associated with data breaches is particularly pernicious due to the fact the information is made available, and has usefulness to identity thieves, for an extended period of time after it is stolen.

83. As a result, victims suffer immediate and long–lasting exposure and are susceptible to further injury over the passage of time.

[31] *See* Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012), available at http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited July 7, 2021).

[32] See Jason Steele, Credit Card and ID Theft Statistics, CreditCards.com (Oct. 23, 2020), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

84. By virtue of the Data Breach and unauthorized release and disclosure of Plaintiffs' and Class members' PII/PHI, Defendant deprived Plaintiffs and Class members of the substantial value of their PII/PHI, to which they are entitled.

85. Recognizing the high value consumers place on their PII/PHI, many companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information they share and who ultimately receives the information. And, by making the transaction transparent, consumers—not criminals—will be compensated.[33]

86. Consumers, such as Plaintiffs and members of the Class, place a high value on their PII and a greater value on their PHI. Research shows how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US $30.49–44.62."[34]

87. As a direct and proximate result of Defendant's wrongful actions, inaction and/or omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and other Class members' PII/PHI, Plaintiffs and the other Class members have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including, *inter alia*, (i) the untimely and inadequate notification of the Data Breach, (ii) the resulting increased risk of future ascertainable losses, economic damages and other actual

[33] *See* Steve Lohr, You Want My Personal Data? Reward Me for It, The New York Times, available at http://www.nytimes.com/2010/07/18/business/18unboxed.html (last visited July 7, 2021).

[34] *See* Il-Horn Hann et al., The Value of Online Information Privacy (Oct. 2002) available at http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited July 7, 2021); *see also* Tsai, Cranor, Acquisti, and Egelman, The Effect of Online Privacy Information on Purchasing Behavior, 22 (2) Information Systems Research 254, 254 (June 2011).

injury and harm, and (iii) the opportunity cost and value of lost time they must spend to monitor their health and financial accounts—for which they are entitled to compensation.

88. As a result of Defendant's failures to prevent the Data Disclosure, Plaintiffs and Class members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft, and/or unauthorized use of their PII/PHI,

b. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud,

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud,

d. The continued risk to their PII/PHI, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the PII/PHI in their possession; and

e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class members.

89. In addition to a remedy for the economic harm, Plaintiffs and the Class Members maintain an undeniable interest in ensuring that their PII/PHI is secure, remains secure, and is not subject to further misappropriation and theft. Plaintiffs therefore requests the injunctive remedies outlined in the Prayer of this Complaint.

CLASS ALLEGATIONS

90. Plaintiffs bring this lawsuit as a class action on behalf of themselves and all others similarly situated as members of the proposed Class pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), 23(b)(3), and 23(c)(4).

91. Plaintiffs seek to represent a proposed Nationwide class defined as follows:

> All persons residing in the United States whose PII/PHI was compromised in the Data Breach that Practice*first* announced on or about June 30, 2021 (the "Class").

92. Excluded from the Class are: (i) Defendant and its officers, directors, affiliates, parents, and subsidiaries (ii) the Judge presiding over this action and the court staff in this case and any members of their immediate families, and (iii) any other person or entity found by a court of competent jurisdiction to be guilty of initiating, causing, aiding or abetting the criminal activity occurrence of the Data Breaches or who pleads nolo contendere to any such charge.

93. Plaintiffs reserve the right to modify or amend the definition of the proposed Class, and/or add subclasses, as additional information becomes available to Plaintiffs. The proposed Class meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

94. Certification of Plaintiffs' claims for class–wide treatment is appropriate because Plaintiffs can prove the elements of her claims on class–wide basis using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

95. **Numerosity**: The members of the Class are so numerous that joinder of all members of the Class is impracticable. Plaintiffs are informed and believe that the proposed Class include 1,210,688 patients and employees who have been damaged by Defendant's conduct as alleged herein.

96. **Commonality**: This action involves common questions of law and fact, which predominate over any questions affecting individual Class members. These common legal and factual questions include, but are not limited to, the following:

a. whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class members' PII/PHI.

b. whether Defendant engaged in the wrongful conduct alleged herein.

c. whether the alleged conduct constitutes violations of the laws asserted.

d. whether Defendant owed Plaintiffs and Class members a duty to adequately protect their PII/PHI.

e. whether Defendant breached its duty to protect Plaintiffs' and Class members' PII/PHI.

f. whether Defendant knew or should have known about the inadequacies of their data protection, storage, and/or physical property security.

g. whether Defendant failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiffs' and Class members' PII/PHI from unauthorized theft, release, disclosure, and/or dissemination.

h. whether the statutorily required and/or industry standard data security measures, policies, procedures, and protocols were in place and operational within Defendant's offices and computer systems to safeguard and protect Plaintiffs' and Class members' PII/PHI from unauthorized theft, release, disclosure and/or dissemination.

i. whether Defendant breached its promise and duty to keep Plaintiffs' and Class members' PII/PHI safe and to follow federal data security protocols.

j. whether Defendant's conduct was the proximate cause of Plaintiffs' and Class members' injuries.

k. whether Defendant took reasonable and timely measures to determine the extent of the Data Breach after it was discovered.

l. whether Plaintiffs and Class members suffered ascertainable and cognizable injuries as a result of Defendant's conduct.

m. whether Plaintiffs and Class members are entitled to recover actual damages; and

n. whether Plaintiffs and Class members are entitled to other appropriate remedies, including injunctive relief.

97. **Predominance:** Defendant engaged in a common course of conduct toward Plaintiffs and Class members, in that Plaintiffs' and Class members' PII/PHI was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendant's conduct affecting Class Members set out in this Complaint predominate over any individualized issues. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

98. **Typicality**: Plaintiffs' claims are typical of the claims of the members of the Class. All Class members were subject to the Data Breach and had their PII/PHI accessed by and/or disclosed to unauthorized third parties. Defendant's misconduct impacted all Class members in the same manner and arose from the same set of operative facts and are based on the same set of legal theories.

99. **Adequacy of Representation**: Plaintiffs will fairly and adequately protect the interests of Class members, have retained counsel experienced in complex consumer class action

litigation—including data privacy class actions, and intend to vigorously prosecute this action. Plaintiffs have no adverse or antagonistic interests to those of the Class.

100. **Superiority**: A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendant. It would thus be virtually impossible for the Class members, on an individual basis, to obtain effective redress for the wrongs done to them. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts and would also increase the delay and expense to all parties and the courts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

101. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class members' names and addresses affected by the Data Breach. Class members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

FIRST CAUSE OF ACTION

NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

102. Plaintiffs incorporate by reference Paragraphs 1 through 101 above as though fully set forth herein.

103. Defendant provides medical management services to medical professionals, and as such Defendant is entrusted with its clients' PII/PHI, including their names, addresses, email addresses, dates of birth, driver's license numbers, Social Security numbers, diagnoses, laboratory and treatment information, patient identification numbers, medication information,

health insurance identification and claims information, tax identification numbers, employee usernames and passwords, employee usernames with security questions and answers, and bank account and/or credit card/debit card information.

104. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between it, its customers and associates, and the patients of its clients, healthcare providers, which is recognized by laws and regulations, including HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class members from a unauthorized access, use, dissemination, and/or exfiltration of the PII/PHI—including data breaches.

105. HIPAA imposes a duty and an actionable standard of care for an ordinary negligence claim. The HIPAA Privacy Rule prohibits covered entities from using or disclosing personal health information, such as the PII/PHI at issue here, except as permitted by regulation. 45 C.F.R. § 164.502(a). The HIPAA privacy restrictions also govern the business associates of covered entities. 45 C.F.R. § 160.102. Practice*first* is subject to the actionable standards of care established by HIPAA as a business associate of covered entities.

106. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

107. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the

unfair practice of failing to use reasonable measures to protect confidential data, including the Plaintiffs' and Class members' PII/PHI. Given Defendant's acute awareness of the sensitivity and privacy concerns surrounding Plaintiffs' and Class members' PII/PHI, Defendant was on notice of the likely consequences from such a breach and the impact it would have on Plaintiffs and Class members.

108. Defendant's duties to protect the PII/PHI arose not only as a result of the statutes and regulations described above, but also because Defendant owed a duty of care to Plaintiffs and Class members to provide data reasonable and adequate security consistent with industry standards, common law, and other requirements discussed herein, to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII/PHI in its custody.

109. Upon receiving the PII/PHI of Plaintiffs and members of the Class, Defendant owed to Plaintiffs and the Class a duty of reasonable care in handling, using, and storing the PII/PHI that included securing and protecting the information from being stolen, accessed, disseminate, and/or misused by unauthorized parties.[35] Pursuant to this duty, Defendant was required to design, maintain, and test its security systems to ensure their systems were reasonably secure and capable of protecting Plaintiffs' and Class members' PII/PHI. Defendant further owed Plaintiffs and Class members a duty to implement systems and procedures capable of detecting unauthorized access to and exfiltration of PII/PHI on their computer systems, including but not limited to a data breach, in a timely manner and to timely act on any security alerts from their systems.

[35] *Wallace v. Health Quest Sys., Inc.*, No. 20 Civ. 545 (VB), 2021 WL 1109727, at *9 (S.D.N.Y. Mar. 23, 2021) (finding that plaintiff plausibly pleaded that an operator of hospitals and healthcare providers owed a duty of care to safeguard customers' and patients' sensitive personal information).

110. Defendant owed this duty to Plaintiffs and the other Class members because Plaintiffs and the other Class members comprise a well–defined, foreseeable, and probable class of individuals whom Defendant should have been aware could and would likely be injured by Defendant' inadequate security protocols. Defendant actively solicited clients who entrusted Defendant with PHI/PHI when obtaining and using Defendant's facilities and services. To facilitate these services, Defendant used, handled, gathered, and stored Plaintiffs' and Class members' PII/PHI. Attendant to Defendant's solicitation, use, and storage, Defendant knew or should have known of its inadequate and unreasonable security practices with regard to its computer/server systems and also knew that hackers and thieves routinely attempt to access, steal, and misuse the PII/PHI Defendant received, used, and stored. As such, Defendant knew a breach of its systems would cause damage to Plaintiffs and the Class members. Thus, Defendant had a duty to act reasonably in protecting the PII/PHI of their clients.

111. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and Class members the scope, nature, and occurrence of the Data Breach. This disclosure is necessary so Plaintiffs and the other Class members can take appropriate measures to avoid unauthorized use of their PII/PHI, accounts, cancel and/or change usernames and passwords on compromised accounts, monitor their accounts to prevent fraudulent activity, contact their financial and/or health institutions and insurance providers about compromise or possible compromise, obtain credit monitoring services, and/or take other steps in an effort to mitigate the harm caused by the Data Breach.

112. Defendant breached its duty and violated HIPAA privacy laws by failing to protect Plaintiffs' and Class members' PII/PHI, provided to Defendant in the normal course and scope of its business practice as a provider of services to healthcare providers. Plaintiffs and

Class members are the exact demographic HIPAA was enacted to protect. As such, the harm incurred as a result of the Data Breach is the type of harm HIPAA was intended to prevent.

113. Defendant breached its duty and violated Section 5 of the FTC Act because it engaged in unfair practices by failing to safeguard Plaintiffs' and Class members' PII/PHI.

114. Defendant breached its duty to Plaintiffs and the Class members by failing to implement and maintain security controls that were capable of adequately protecting the PII/PHI entrusted to it.

115. Defendant breached its duty to Plaintiffs and the Class members by failing to monitor its computer systems and/or implement and maintain security controls that would timely detect and notify Defendant of unauthorized access to the PII/PHI entrusted to it.

116. Defendant also breached its duty to timely and accurately disclose to Plaintiffs and the Class members that their PII/PHI had been, or was reasonably believed to have been, improperly accessed, disseminated and/or stolen. Plaintiffs and Class members had no way to protect their PII/PHI in Defendant's possession.

117. Defendant's breach of its duties and failure to take reasonable steps to protect Plaintiffs' and Class members' PII/PHI was a proximate cause of Plaintiffs' and Class members' injuries because Defendant's acts and omissions regarding implementation of reasonable and adequate computer security measures directly allowed thieves easy access to Plaintiffs' and Class members' PII/PHI. This ease of access allowed thieves to access, view, and steal Plaintiffs' and Class members' PII/PHI, which leads to identity theft and fraud charges.[36]

118. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class members have suffered theft of their PII/PHI. Defendant allowed thieves access and exfiltrate

[36] *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015) ("Why else would hackers . . . steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities.")

Plaintiffs' and Class members' PII/PHI, thereby decreasing the security of Plaintiffs' and Class members' financial and health accounts, making their identities less secure and reliable, and subjecting them to the imminent threat of identity theft and other fraudulent acts. Not only will Plaintiffs and Class members have to incur time and money to mitigate damages and attempt to prevent injuries and damages by—to the extent possible—re–securing their bank accounts/health insurance accounts, medical records, and identities, but because much of PII/PHI is not subject to (or is difficult to) change, Plaintiffs and Class members will also have to protect against identity theft for years to come.

119. It was foreseeable that Defendant's failure to use adequate, reasonable, and commercially available measures to protect Plaintiffs' and Class members' PII/PHI would result in injury to Plaintiffs and Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in both the financial services and medical industries.

120. The injuries to Plaintiffs and Class members were reasonably foreseeable to Defendant because laws and statutes, and industry standards require Defendant to safeguard and protect its computer systems and employ procedures and controls to ensure that unauthorized third parties did not gain access to Plaintiffs' and the Class members' PII/PHI.

121. The injuries to Plaintiffs and the other Class members also were reasonably foreseeable because Defendant knew or should have known that its systems used for safeguarding PII/PHI were inadequately secured and exposed Plaintiffs' and Class members' PII/PHI to being breached, accessed, and stolen by hackers and unauthorized third parties. As such, Defendant's own misconduct allowed the data breach and created foreseeable risk of harm to Plaintiffs and Class members.

122. Plaintiffs and Class members have suffered and/or will suffer injury and damages, including but not limited to:

a. the loss of the benefit of their bargain with Defendant.

b. the publication and/or theft of their PII/PHI.

c. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII/PHI.

d. lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft.

e. costs associated with placing freezes on credit reports.

f. anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

g. the continued risk to their PII/PHI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII/PHI of Plaintiffs and Class members in its continued possession; and,

h. future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII/PHI for the rest of their lives.

123. Defendant's conduct warrants moral blame because Defendant actively offered services to the healthcare industry, wherein it used, handled, processed, and stored the PII/PHI of Plaintiffs and the Class members without disclosing that their security was inadequate and unable to protect PII/PHI. Holding Defendant accountable for its negligence will further the

policies embodied in such law by incentivizing larger healthcare industry professionals and medical service providers to properly secure sensitive patient information and protect the patients who rely on these companies and place their lives in their hands every day.

124. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

125. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to Plaintiffs and Class members.

SECOND CAUSE OF ACTION

BREACH OF CONTRACTS TO WHICH PLAINTIFFS ARE THIRD PARTY BENEFICIARIES

(On Behalf of the Plaintiffs and the Class)

126. Plaintiffs incorporate by reference Paragraphs 1 through 101 above as though fully set forth herein.

127. Defendant had express or implied contracts or agreements with several medical providers and other medical entities to provide services including secure patient data and records management, retention, retrieval, and storage.

128. Plaintiffs and Class members are intended third–party beneficiaries of contracts entered into between Defendant and these medical entities because it is Plaintiffs' and Class members' PII/PHI that is one of the subjects of the contracts and for which Defendant agreed to provide secure patient billing, credentialing, coding, compliance, chart auditing, bookkeeping, and/or tax preparation services.

129. As previously alleged, Defendant breached these contracts by failing to provide secure or adequate data storage services, resulting in the Data Breach and the theft and misuse of

the PII/PHI of Plaintiffs and the Class by unauthorized third persons.

130. Plaintiffs and Class members have a right to recovery for breach of the contracts because one or more of the parties to these contracts intended to give Plaintiffs and Class members the benefit of the performance promised in the contracts.

131. As a direct and proximate result of Defendant's breaches of these contracts, Plaintiffs and Class members suffered the injuries previously described in detail.

132. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of Defendant's breach.

133. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to Plaintiffs and Class members.

THIRD CAUSE OF ACTION

DECLARATORY AND INJUNCTIVE RELIEF

(On Behalf of the Plaintiffs and the Class)

134. Plaintiffs incorporate by reference Paragraphs 1 through 101 as though fully set forth herein.

135. As previously alleged, Defendant owed duties of care to Plaintiffs and Class members requiring Defendant to adequately secure the PII/PHI entrusted to them.

136. Defendant still possess Plaintiffs' and Class members' PII/PHI.

137. Defendant has not fully remedied the vulnerabilities in its practices, procedures, and policies regarding ensuring the data security of Plaintiffs' and Class members' PII/PHI.

138. Accordingly, Defendant has not satisfied its legal obligations and duties to Plaintiffs and the Class members. On the contrary, now that Defendant's vulnerabilities and lax

approach towards data security has become public, the PII/PHI in its possession is more vulnerable than it was prior to announcement of the Data Breach.

139. Actual harm has arisen in the wake of the Data Breach regarding Defendant's obligations and duties of care to provide data security measures to Plaintiffs and the Class members.

140. Plaintiffs, therefore, seek a declaration that Defendant's existing data security measures do not comply with their obligations and duties of care, and to comply with its obligations and duties of care, Defendant must implement and maintain reasonable security measures, including those set forth in the prayer below.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually, and on behalf of all others similarly situated, respectfully requests that the Court enter an order:

a. Certifying the Class as requested herein.

b. Appointing Plaintiffs as Class Representative and undersigned counsel as Class Counsel.

c. Finding that Defendant engaged in the unlawful conduct as alleged herein.

d. Enjoining Defendant's conduct and requiring Defendant to implement proper data security practices, specifically:

   i. prohibiting Defendant from engaging in the wrongful acts described herein.

   ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and laws.

iii. requiring Defendant to delete, destroy, and purge the PII/PHI of Plaintiffs and the Class members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and the Class members.

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiffs' and the Class members' PII/PHI.

v. requiring Defendant to engage independent third–party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on periodic bases, and ordering Defendant to promptly correct any problems or issues detected by such third–party security auditors.

vi. requiring Defendant to engage independent third–party security auditors and internal personnel to run automated security monitoring.

vii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures.

viii. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems.

ix. requiring Defendant to conduct regular database scanning and securing checks.

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII/PHI, as well as protecting the PII/PHI of Plaintiffs and the Class members.

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

xii. requiring Defendant to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting PII/PHI.

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated.

xiv. requiring Defendant to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential PII/PHI to third parties, as well as the steps affected individuals must take to protect themselves.

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from its servers.

xvi. requiring Defendant to design, maintain, and test their computer systems to ensure PII/PHI in its possession is adequately secured and protected.

xvii. requiring Defendant to disclose any future data breaches in a timely and accurate manner.

xviii. requiring Defendant to implement multi–factor authentication requirements, consistent with best practices.

xix. requiring Defendant's employees to change their passwords on a timely and regular basis, consistent with best practices; and

xx. requiring Defendant to provide lifetime credit monitoring and identity theft repair services to Plaintiffs and Class members.

e. Awarding Plaintiffs and Class members damages.

f. Awarding Plaintiffs and Class members pre-judgment and post-judgment interest on all amounts awarded.

g. Awarding Plaintiffs and the Class members reasonable attorneys' fees, costs, and expenses; and

h. Granting such other relief as the Court deems just and proper.

JURY TRIAL DEMANDED

Plaintiffs, on behalf of themselves and the Class, demand a trial by jury on all issues so triable.

Respectfully Submitted,

Dated: October 21, 2021

Gary S. Graifman
KANTROWITZ, GOLDHAMER & GRAIFMAN, P.C.

747 Chestnut Ridge Road
Chestnut Ridge, NY 10977
Telephone: (800) 711-5258
ggraifman@kgglaw.com

Gary E. Mason
David K. Lietz, *Pro Hac Vice*
MASON LIETZ & KLINGER LLP
5301 Wisconsin Avenue, NW, Suite 305
Washington, DC 20016
Tel: (202) 429-2290
gmason@masonllp.com
dlietz@masonllp.com

Todd S. Garber, Esq.
FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP
One North Broadway, Suite 900
White Plains, NY 10601
Tel: (914) 298-3283
www.fbfglaw.com

Gayle M. Blatt, *Pro Hac Vice*
CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP
110 Laurel Street
San Diego, CA 92101
Telephone: (619) 238-1811
Facsimile: (619) 544-9232
gmb@cglaw.com

Counsel for Plaintiffs and the Class